

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

<https://www.2passeasy.com/dumps/Identity-and-Access-Management-Architect/>



NEW QUESTION 1

Universal containers(UC) has implemented SAML-BASED single Sign-on for their salesforce application and is planning to provide access to salesforce on mobile devices using the salesforce1 mobile app. UC wants to ensure that single Sign-on is used for accessing the salesforce1 mobile app. Which two recommendations should the architect make? Choose 2 answers

- A. Use the existing SAML SSO flow along with user agent flow.
- B. Configure the embedded Web browser to use my domain URL.
- C. Use the existing SAML SSO flow along with Web server flow
- D. Configure the salesforce1 app to use the my domain URL

Answer: BD

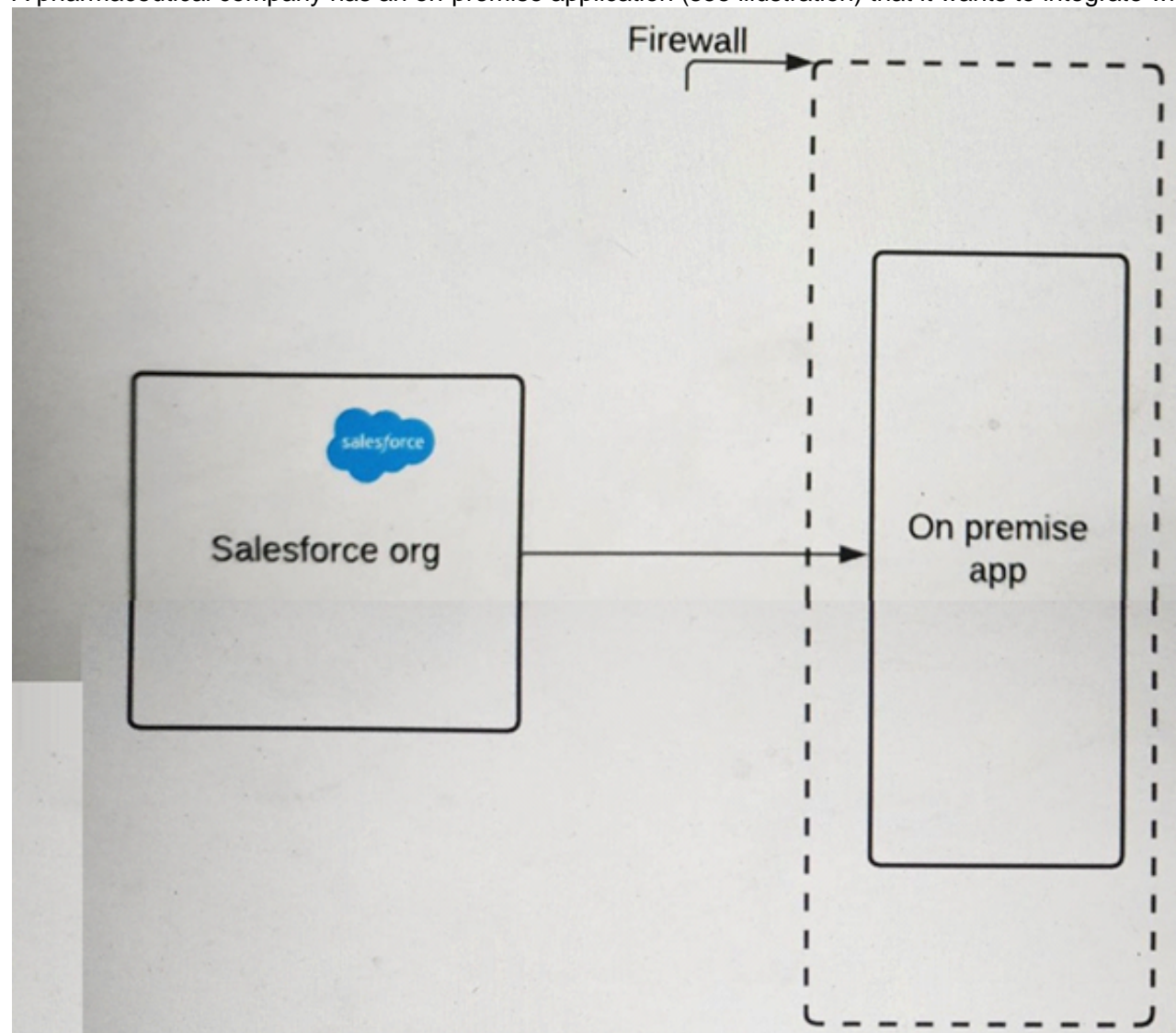
Explanation:

To use SAML SSO for accessing the Salesforce1 mobile app, the architect should recommend configuring the embedded web browser to use the My Domain URL and configuring the Salesforce1 app to use the My Domain URL. Using the My Domain URL allows Salesforce to identify the identity provider and initiate the SSO process. Using the existing SAML SSO flow along with user agent flow or web server flow is not necessary because Salesforce Mobile Applications only work with service provider initiated setups. Therefore, option B and D are the correct answers.

References: Salesforce Mobile Application Single Sign-On overview, SAML SSO with Salesforce as the Service Provider, Single Sign-On

NEW QUESTION 2

A pharmaceutical company has an on-premise application (see illustration) that it wants to integrate with Salesforce.



The IT director wants to ensure that requests must include a certificate with a trusted certificate chain to access the company's on-premise application endpoint. What should an Identity architect do to meet this requirement?

- A. Use open SSL to generate a Self-signed Certificate and upload it to the on-premise app.
- B. Configure the company firewall to allow traffic from Salesforce IP ranges.
- C. Generate a certificate authority-signed certificate in Salesforce and uploading it to the on-premise application Truststore.
- D. Upload a third-party certificate from Salesforce into the on-premise server.

Answer: C

Explanation:

To ensure that requests must include a certificate with a trusted certificate chain to access the company's on-premise application endpoint, the identity architect should generate a certificate authority-signed certificate in Salesforce and upload it to the on-premise application Truststore. A certificate authority-signed certificate is a certificate that is issued by a trusted third-party entity, such as VeriSign or Thawte, that verifies the identity and authenticity of the certificate holder. A Truststore is a repository that stores trusted certificates and public keys. By generating a certificate authority-signed certificate in Salesforce and uploading it to the on-premise application Truststore, the identity architect can enable mutual authentication and secure communication between Salesforce and the on-premise application. The other options are not recommended for this scenario, as they either do not provide a trusted certificate chain, do not enable mutual authentication, or do not secure the communication. References: Create Certificate Authority-Signed Certificates, Mutual Authentication

NEW QUESTION 3

Which three are features of federated Single sign-on solutions? Choose 3 Answers

- A. It establishes trust between Identity Store and Service Provider.
- B. It federates credentials control to authorized applications.

- C. It solves all identity and access management problems.
- D. It improves affiliated applications adoption rates.
- E. It enables quick and easy provisioning and deactivating of users.

Answer: ADE

Explanation:

The three features of federated single sign-on (SSO) solutions are:

- It establishes trust between identity store and service provider. Federated SSO is a process that allows users to access multiple applications or systems with one set of credentials by using a common identity provider (IdP) that authenticates the user and issues a security token to the service provider (SP) that grants access. This process requires a trust relationship between the IdP and the SP, which is established by exchanging metadata and certificates.
 - It improves affiliated applications adoption rates. Federated SSO improves the user experience and satisfaction by reducing the number of login prompts, passwords, and authentication failures that users have to deal with when accessing multiple applications or systems. This can increase the usage and adoption rates of the affiliated applications or systems, as users can access them more easily and conveniently.
 - It enables quick and easy provisioning and deprovisioning of users. Federated SSO enables centralized management of user accounts and access rights by using the IdP as the source of truth for user identity and attributes. This can simplify and automate the provisioning and deprovisioning of users across multiple applications or systems, as changes made in the IdP can be reflected in the SPs without requiring manual intervention or synchronization.
- The other option is not a feature of federated SSO solutions. Federated SSO does not solve all identity and access management problems, as it still faces challenges such as security risks, compatibility issues, governance policies, and user education. References: [Federated Single Sign-On], [Set Up Federated Authentication Using SAML], [Benefits of Single Sign-On], [How Single Sign-On Improves Application Adoption Rates], [User Provisioning for Federated Single Sign-On], [Just-in-Time Provisioning for SAML], [Challenges of Single Sign-On]

NEW QUESTION 4

Universal Containers (UC) is building an authenticated Customer Community for its customers. UC does not want customer credentials stored in Salesforce and is confident its customers would be willing to use their social media credentials to authenticate to the community. Which two actions should an Architect recommend UC to take?

- A. Use Delegated Authentication to call the Twitter login API to authenticate users.
- B. Configure an Authentication Provider for LinkedIn Social Media Accounts.
- C. Create a Custom Apex Registration Handler to handle new and existing users.
- D. Configure SSO Settings For Facebook to serve as a SAML Identity Provider.

Answer: BC

Explanation:

Configuring an Authentication Provider for LinkedIn Social Media Accounts allows UC to use LinkedIn as an external identity provider for its customer community. This means that customers can use their LinkedIn credentials to log in to the community without storing their credentials in Salesforce. Creating a Custom Apex Registration Handler allows UC to customize how new and existing users are handled when they log in with an external identity provider. This means that UC can control how user records are created, updated, or matched when customers use their social media credentials to authenticate to the community. These two actions can meet the requirement of UC to use social media credentials for its customer community.

NEW QUESTION 5

A Salesforce customer is implementing Sales Cloud and a custom pricing application for its call center agents. An Enterprise single sign-on solution is used to authenticate and sign-in users to all applications. The customer has the following requirements:

- * 1. The development team has decided to use a Canvas app to expose the pricing application to agents.
- * 2. Agents should be able to access the Canvas app without needing to log in to the pricing application.

Which two options should the identity architect consider to provide support for the Canvas app to initiate login for users?
Choose 2 answers

- A. Select "Enable as a Canvas Personal App" in the connected app settings.
- B. Enable OAuth settings in the connected app with required OAuth scopes for the pricing application.
- C. Configure the Canvas app as a connected app and set Admin-approved users as pre-authorized.
- D. Enable SAML in the connected app and Security Assertion Markup Language (SAML) Initiation Method as Service Provider Initiated.

Answer: CD

Explanation:

To allow agents to access the Canvas app without needing to log in to the pricing application, the identity architect should consider two options:

- Configure the Canvas app as a connected app and set Admin-approved users as pre-authorized. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols. A Canvas app is a type of connected app that allows an external application to be embedded within Salesforce. By setting Admin-approved users as pre-authorized, the identity architect can control which users can access the Canvas app by assigning profiles or permission sets to the connected app.
 - Enable SAML in the connected app and Security Assertion Markup Language (SAML) Initiation Method as Service Provider Initiated. SAML is a protocol that allows users to authenticate and authorize with an external identity provider and access Salesforce resources. By enabling SAML in the connected app, the identity architect can use Salesforce as a service provider (SP) and the pricing application as an identity provider (IdP) for single sign-on (SSO). By setting SAML Initiation Method as Service Provider Initiated, the identity architect can initiate the SSO process from Salesforce and send a SAML request to the pricing application.
- References: Connected Apps, Canvas Apps, SAML Single Sign-On Settings

NEW QUESTION 6

Universal Containers is considering using Delegated Authentication as the sole means of Authenticating of Salesforce users. A Salesforce Architect has been brought in to assist with the implementation. What two risks Should the Architect point out? Choose 2 answers

- A. Delegated Authentication is enabled or disabled for the entire Salesforce org.
- B. UC will be required to develop and support a custom SOAP web service.
- C. Salesforce users will be locked out of Salesforce if the web service goes down.
- D. The web service must reside on a public cloud service, such as Heroku.

Answer: BC

Explanation:

The two risks that the architect should point out for using delegated authentication as the sole means of authenticating Salesforce users are:

- UC will be required to develop and support a custom SOAP web service. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This feature requires UC to develop and support a custom SOAP web service that can accept and validate the user's username and password, and return a boolean value to indicate whether the authentication is successful or not. This could increase complexity and cost for UC, as they need to write custom code and maintain the web service.
- Salesforce users will be locked out of Salesforce if the web service goes down. Delegated authentication relies on the availability and performance of the external web service that handles the authentication requests from Salesforce. If the web service goes down or becomes slow, Salesforce users will not be able to log in or access Salesforce, as they will receive an error message or a timeout response. This could cause disruption and frustration for UC's business operations and user satisfaction.

The other options are not valid risks for using delegated authentication. Delegated authentication can be enabled or disabled for individual users or groups of users by using permission sets or profiles, not for the entire Salesforce org. The web service does not need to reside on a public cloud service, such as Heroku, as it can be hosted on any platform that supports SOAP services and can communicate with Salesforce. References: [Delegated Authentication], [Enable 'Delegated Authentication'], [Troubleshoot Delegated Authentication]

NEW QUESTION 7

A large consumer company is planning to create a community and will require login through the customer's social identity. The following requirements must be met:

- * 1. The customer should be able to login with any of their social identities, however Salesforce should only have one user per customer.
- * 2. Once the customer has been identified with a social identity, they should not be required to authorize Salesforce.
- * 3. The customer's personal details from the social sign-on need to be captured when the customer logs into Salesforce using their social identity.
- * 3. If the customer modifies their personal details in the social site, the changes should be updated in Salesforce.

Which two options allow the Identity Architect to fulfill the requirements? Choose 2 answers

- A. Use Login Flows to call an authentication registration handler to provision the user before logging the user into the community.
- B. Use authentication providers for social sign-on and use the custom registration handler to insert or update personal details.
- C. Redirect the user to a custom page that allows the user to select an existing social identity for login.
- D. Use the custom registration handler to link social identities to Salesforce identities.

Answer: BD

Explanation:

To allow customers to log in to the community with any of their social identities, such as Facebook, Google, or Twitter, the identity architect needs to use authentication providers for social sign-on. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. To ensure that Salesforce has only one user per customer, regardless of how many social identities they have, the identity architect needs to use the custom registration handler to link social identities to Salesforce identities. The custom registration handler is a class that implements the Auth.RegistrationHandler interface and defines how to create or update users in Salesforce based on the information from the external identity provider. The custom registration handler can also be used to insert or update personal details of the customers when they log in to Salesforce using their social identity.

References: Authentication Providers, Social Sign-On with Authentication Providers, Create a Custom Registration Handler

NEW QUESTION 8

Universal Containers (UC) has a desktop application to collect leads for marketing campaigns. UC wants to extend this application to integrate with Salesforce to create leads. Integration between the desktop application and Salesforce should be seamless. What Authorization flow should the Architect recommend?

- A. JWT Bearer Token Flow
- B. Web Server Authentication Flow
- C. User Agent Flow
- D. Username and Password Flow

Answer: B

Explanation:

This is an OAuth authorization flow that allows a web server application to obtain an access token to access Salesforce resources on behalf of the user¹. This flow is suitable for integrating a desktop application with Salesforce, as it does not require the user to enter their credentials in the application, but rather redirects them to the Salesforce login page to authenticate and authorize the application². This way, the integration between the desktop application and Salesforce is seamless and secure. The other options are not optimal for this requirement because:

- JWT Bearer Token Flow is an OAuth authorization flow that allows a client application to obtain an access token by sending a signed JSON Web Token (JWT) to Salesforce³. This flow does not involve user interaction, and requires the client application to have a certificate and a private key to sign the JWT. This flow is more suitable for server-to-server integration, not for desktop application integration.
- User Agent Flow is an OAuth authorization flow that allows a user-agent-based application (such as a browser or a mobile app) to obtain an access token by redirecting the user to Salesforce and receiving the token in the URL fragment⁴. This flow is not suitable for desktop application integration, as it requires the application to parse the URL fragment and store the token securely.
- Username and Password Flow is an OAuth authorization flow that allows a client application to obtain an access token by sending the user's username and password to Salesforce⁵. This flow is not recommended for desktop application integration, as it requires the user to enter their credentials in the application, which is not secure or seamless. References: OAuth Authorization Flows, Implement the OAuth 2.0 Web Server Flow, JWT-Based Access Tokens (Beta), User-Agent Flow, Username-Pass Flow

NEW QUESTION 9

A global company's Salesforce Identity Architect is reviewing its Salesforce production org login history and is seeing some intermittent Security Assertion Markup Language (SAML SSO) 'Replay Detected and Assertion Invalid' login errors.

Which two issues would cause these errors?

Choose 2 answers

- A. The subject element is missing from the assertion sent to Salesforce.
- B. The certificate loaded into SSO configuration does not match the certificate used by the IdP.
- C. The current time setting of the company's identity provider (IdP) and Salesforce platform is out of sync by more than eight minutes.
- D. The assertion sent to Salesforce contains an assertion ID previously used.

Answer: CD

Explanation:

A SAML SSO 'Replay Detected and Assertion Invalid' error occurs when Salesforce detects that the same assertion has been used more than once within the validity period. This can happen if the assertion ID is reused by the IdP or if the assertion is resent by the user. Another possible cause is that the time settings of the IdP and Salesforce are not synchronized, which can result in an assertion being valid for a shorter or longer period than expected. References: SAML Single Sign-On Settings, Troubleshoot SAML Single Sign-On

NEW QUESTION 10

Containers (UC) uses an internal system for recruiting and would like to have the candidates' info available in the Salesforce automatically when they are selected. UC decides to use OAuth to connect to Salesforce from the recruiting system and would like to do the authentication using digital certificates. Which two OAuth flows should be considered to meet the requirement? Choose 2 answers

- A. JWT Bearer Token flow
- B. Refresh Token flow
- C. SAML Bearer Assertion flow
- D. Web Service flow

Answer: AC

Explanation:

JWT Bearer Token flow and SAML Bearer Assertion flow are two OAuth flows that can be used to authenticate to Salesforce using digital certificates. JWT Bearer Token flow allows a connected app to request an access token from Salesforce by using a JSON Web Token (JWT) that is signed with a digital certificate. SAML Bearer Assertion flow allows a connected app to request an access token from Salesforce by using a SAML assertion that is signed with a digital certificate. These two flows can meet the requirement of UC to use OAuth and digital certificates to connect to Salesforce from the recruiting system.

NEW QUESTION 10

Universal Containers (UC) wants to provide single sign-on (SSO) for a business-to-consumer (B2C) application using Salesforce Identity. Which Salesforce license should UC utilize to implement this use case?

- A. Identity Only
- B. Salesforce Platform
- C. External Identity
- D. Partner Community

Answer: C

Explanation:

External Identity is the license that enables SSO for B2C applications using Salesforce Identity. It also provides self-registration, social sign-on, and user profile management features. References: Certification - Identity and Access Management Architect - Trailhead

NEW QUESTION 15

Universal Containers is creating a web application that will be secured by Salesforce Identity using the OAuth 2.1 Web Server Flow uses the OAuth 2.0 authorization code grant type). Which three OAuth concepts apply to this flow? Choose 3 answers

- A. Verification URL
- B. Client Secret
- C. Access Token
- D. Scopes

Answer: BCD

Explanation:

The OAuth 2.0 Web Server Flow requires the client secret to authenticate the web application to Salesforce. The access token is used to access the Salesforce resources on behalf of the user. The scopes define the permissions and access levels for the web application. References: OAuth 2.0 Web Server Authentication Flow, Digging Deeper into OAuth 2.0 on Force.com

NEW QUESTION 20

An identity architect has built a native mobile application and plans to integrate it with a Salesforce Identity solution. The following are the requirements for the solution:

- * 1. Users should not have to login every time they use the app.
- * 2. The app should be able to make calls to the Salesforce REST API.
- * 3. End users should NOT see the OAuth approval page.

How should the identity architect configure the Salesforce connected app to meet the requirements?

- A. Enable the API Scope and Offline Access Scope, upload a certificate so JWT Bearer Flow can be used and then set the connected app access settings to "Admin Pre-Approved".
- B. Enable the API Scope and Offline Access Scope on the connected app, and then set the connected app to access settings to 'Admin Pre-Approved'.
- C. Enable the Full Access Scope and then set the connected app access settings to "Admin Pre-Approved".
- D. Enable the API Scope and Offline Access Scope on the connected app, and then set the Connected App access settings to "User may self authorize".

Answer: A

Explanation:

JWT Bearer Flow is an OAuth 2.0 flow that allows a client app to obtain an access token without user interaction. It requires a certificate to sign the JWT and the API and Offline Access scopes to access the Salesforce REST API and refresh the token. The connected app must also be pre-approved by the admin to avoid the OAuth approval page. References: OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration, Authorize an Org Using the JWT Flow

NEW QUESTION 21

Universal Containers (UC) is building a customer community and will allow customers to authenticate using Facebook credentials. The First time the user authenticating using Facebook, UC would like a customer account created automatically in their accounting system. The accounting system has a web service accessible to Salesforce for the creation of accounts. How can the Architect meet these requirements?

- A. Create a custom application on Heroku that manages the sign-on process from Facebook.
- B. Use JIT Provisioning to automatically create the account in the accounting system.
- C. Add an Apex callout in the registration handler of the authorization provider.
- D. Use OAuth JWT flow to pass the data from Salesforce to the Accounting System.

Answer: C

Explanation:

The best option for UC to meet the requirements is to add an Apex callout in the registration handler of the authorization provider. An authorization provider is a configuration in Salesforce that allows users to log in with an external authentication provider, such as Facebook. A registration handler is an Apex class that implements the Auth.RegistrationHandler interface and defines the logic for creating or updating a user account when a user logs in with an external authentication provider. An Apex callout is a method that invokes an external web service from Apex code. By adding an Apex callout in the registration handler, UC can create a customer account in their accounting system by calling the web service that is accessible to Salesforce. This option enables UC to automate the account creation process and integrate with their existing accounting system. The other options are not optimal for this scenario. Creating a custom application on Heroku that manages the sign-on process from Facebook would require UC to develop and maintain a separate application and infrastructure, which could increase complexity and cost. Using JIT provisioning to automatically create the account in the accounting system would require UC to configure Facebook as a SAML identity provider, which is not supported by Facebook. Using OAuth JWT flow to pass the data from Salesforce to the accounting system would require UC to obtain an OAuth token from the accounting system and use it to make API calls, which could introduce security and performance issues. References: [Authorization Providers], [Create a Registration Handler Class], [Auth.RegistrationHandler Interface], [Apex Callouts], [Facebook as SAML Identity Provider], [OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration]

NEW QUESTION 22

A web service is developed that allows secure access to customer order status on the Salesforce Platform. The service connects to Salesforce through a connected app with the web server flow. The following are the required actions for the authorization flow:

- * 1. User Authenticates and Authorizes Access
- * 2. Request an Access Token
- * 3. Salesforce Grants an Access Token
- * 4. Request an Authorization Code
- * 5. Salesforce Grants Authorization Code

What is the correct sequence for the authorization flow?

- A. 1, 4, 5, 2, 3
- B. 4, 1, 5, 2, 3
- C. 2, 1, 3, 4, 5
- D. 4,5,2, 3, 1

Answer: B

Explanation:

The web server flow is an OAuth 2.0 authorization code grant type, which follows this sequence of steps:

- The client app requests an authorization code from Salesforce by redirecting the user to the authorization endpoint.
- The user authenticates and authorizes access to the client app.
- Salesforce grants an authorization code and redirects the user back to the client app.
- The client app requests an access token from Salesforce by sending the authorization code to the token endpoint.
- Salesforce grants an access token and a refresh token to the client app. References: OAuth Authorization Flows, Authorize Apps with OAuth

NEW QUESTION 23

How should an Architect automatically redirect users to the login page of the external Identity provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider?

- A. Use visualforce as the landing page for My Domain to redirect users to the Identity Provider login Page.
- B. Enable the Redirect to the Identity Provider setting under Authentication Services on the My domainConfiguration.
- C. Remove the Login page from the list of Authentication Services on the My Domain configuration.
- D. Set the Identity Provider as default and enable the Redirect to the Identity Provider setting on the SAML Configuration.

Answer: D

Explanation:

Setting the Identity Provider as default and enabling the Redirect to the Identity Provider setting on the SAML Configuration will automatically redirect users to the login page of the external Identity Provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider¹. Option A is incorrect because Visualforce is not a supported method for redirecting users to the Identity Provider login page². Option B is incorrect because enabling the Redirect to the Identity Provider setting under Authentication Services on the My Domain Configuration will only redirect users to the Identity Provider login page when using an IdP-Initiated SAML flow³. Option C is incorrect because removing the Login page from the list of Authentication Services on the My Domain configuration will not affect the SP-Initiated SAML flow, and may cause other issues with authentication⁴.

References: SAML SSO Flows, Set up a Service Provider initiated login flow, Configure SAML single sign-on with an identity provider, SAML Identity Provider Configuration Settings

NEW QUESTION 26

Universal containers (UC) is setting up their customer Community self-registration process. They are uncomfortable with the idea of assigning new users to a default account record. What will happen when customers self-register in the community?

- A. The self-registration process will produce an error to the user.
- B. The self-registration page will ask user to select an account.

- C. The self-registration process will create a person Account record.
- D. The self-registration page will create a new account record.

Answer: C

Explanation:

When customers self-register in the community, the self-registration process will create a person account record. A person account is a special type of account that combines both account and contact information in one record. This allows customers to have their own individual accounts without being associated with a default account. Option A is not a good choice because the self-registration process will not produce an error to the user, unless there is some configuration or validation issue. Option B is not a good choice because the self-registration page will not ask user to select an account, unless it is customized to do so. Option D is not a good choice because the self-registration page will not create a new account record, unless it is customized to do so.
References: [How to Provision Salesforce Communities Users], [Salesforce Licensing]

NEW QUESTION 27

Northern Trail Outfitters (NTO) believes a specific user account may have been compromised. NTO inactivated the user account and needs U perform a forensic analysis and identify signals that could Indicate a breach has occurred.
What should NTO's first step be in gathering signals that could indicate account compromise?

- A. Review the User record and evaluate the login and transaction history.
- B. Download the Setup Audit Trail and review all recent activities performed by the user.
- C. Download the Identity Provider Event Log and evaluate the details of activities performed by the user.
- D. Download the Login History and evaluate the details of logins performed by the user.

Answer: D

Explanation:

The Experience ID is a unique identifier for each Experience Cloud site that can be used to customize the branding and user interface based on the OAuth/Open ID or SAML flows. The Experience ID can be passed as a URL parameter to Salesforce to determine which site the user is accessing. References: Experience ID, Customize Your Experience Cloud Site Login Process

NEW QUESTION 30

Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for to give its customers the ability to login with their Facebook and Twitter credentials.
Which two actions should an identity architect recommend to meet these requirements? Choose 2 answers

- A. Create a custom external authentication provider for Facebook.
- B. Configure a predefined authentication provider for Facebook.
- C. Create a custom external authentication provider for Twitter.
- D. Configure a predefined authentication provider for Twitter.

Answer: BD

Explanation:

To give customers the ability to login with their Facebook and Twitter credentials, the identity architect should configure a predefined authentication provider for Facebook and a predefined authentication provider for Twitter. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and Twitter, which can be easily configured with minimal customization. Creating a custom external authentication provider is not necessary for this scenario. References: Authentication Providers, Social Sign-On with Authentication Providers

NEW QUESTION 32

An architect needs to advise the team that manages the identity provider how to differentiate salesforce from other service providers. What SAML SSO setting in salesforce provides this capability?

- A. Entity id
- B. Issuer
- C. Identity provider login URL
- D. SAML identity location

Answer: A

Explanation:

The Entity ID is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity ID is a unique identifier for the service provider that is sent in the SAML request and response messages¹. The identity provider uses the Entity ID to determine which service provider is requesting or receiving authentication information². You can customize the Entity ID for your Salesforce org or Experience Cloud site in the SAML Single Sign-On Settings page³. References: 1: SAML SSO Flows 2: Federated Authentication Using SAML to Log in to Salesforce Org 3: Step 2: Create a SA Single Sign-On Setting in Salesforce

NEW QUESTION 37

An insurance company has a connected app in its Salesforce environment that is used to integrate with a Google Workspace (formerly knot as G Suite). An identity and access management (IAM) architect has been asked to implement automation to enable users, freeze/suspend users, disable users, and reactivate existing users in Google Workspace upon similar actions in Salesforce.
Which solution is recommended to meet this requirement?

- A. Configure user Provisioning for Connected Apps.
- B. Update the Security Assertion Markup Language Just-in-Time (SAML JIT) handler in Salesforce for user provisioning and de-provisioning.
- C. Build a custom REST endpoint in Salesforce that Google Workspace can poll against.
- D. Build an Apex trigger on the userlogin object to make asynchronous callouts to Google APIs.

Answer: A

Explanation:

User Provisioning for Connected Apps allows Salesforce to create, update, and deactivate users in an external service such as Google Workspace based on user and permission set assignments in Salesforce. References: User Provisioning for Connected Apps

NEW QUESTION 40

Northern Trail Outfitters (NTO) wants to improve its engagement with existing customers to boost customer loyalty. To get a better understanding of its customers, NTO establishes a single customer view including their buying behaviors, channel preferences and purchasing history. All of this information exists but is spread across different systems and formats.

NTO has decided to use Salesforce as the platform to build a 360 degree view. The company already uses Microsoft Active Directory (AD) to manage its users and company assets.

What should an Identity Architect do to provision, deprovision and authenticate users?

- A. Salesforce Identity is not needed since NTO uses Microsoft AD.
- B. Salesforce Identity can be included but NTO will be required to build a custom integration with Microsoft AD.
- C. Salesforce Identity is included in the Salesforce licenses so it does not need to be considered separately.
- D. A Salesforce Identity can be included but NTO will require Identity Connect.

Answer: D

Explanation:

Identity Connect is a Salesforce product that integrates Microsoft Active Directory with Salesforce user records. It allows provisioning, deprovisioning, and authentication of users based on AD data. The other options are either incorrect or irrelevant for this use case. References: Get to Know Identity Connect, Identity Connect

NEW QUESTION 41

Universal containers (UC) wants users to authenticate into their salesforce org using credentials stored in a custom identity store. UC does not want to purchase or use a third-party Identity provider. Additionally, UC is extremely wary of social media and does not consider it to be trust worthy. Which two options should an architect recommend to UC? Choose 2 answers

- A. Use a professional social media such as LinkedIn as an Authentication provider
- B. Build a custom web page that uses the identity store and calls frontdoor.jsp
- C. Build a custom Web service that is supported by Delegated Authentication.
- D. Implement the OpenID protocol and configure an authentication provider

Answer: CD

Explanation:

The two options that an architect should recommend to UC are to build a custom web service that is supported by delegated authentication and to implement the OpenID protocol and configure an authentication provider. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service instead of using Salesforce credentials³. A custom web service can be built to use the credentials stored in the custom identity store and validate them against Salesforce using SOAP or REST API³. OpenID is an open standard protocol that allows users to authenticate with various web services using an existing account⁴. An authentication provider can be configured in Salesforce to use OpenID and connect with the custom identity store⁵.

References: Delegated Authentication, OpenID, Authentication Providers

NEW QUESTION 44

Universal containers (UC) uses a legacy Employee portal for their employees to collaborate and post their ideas. UC decides to use salesforce ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to push ideas posted on the Employee portal to salesforce through API. UC decides to use an API user using OAuth Username - password flow for the connection. How can the connection to salesforce be restricted only to the employee portal server?

- A. Add the Employee portals IP address to the Trusted IP range for the connected App
- B. Use a digital certificate signed by the employee portal Server.
- C. Add the employee portals IP address to the login IP range on the user profile.
- D. Use a dedicated profile for the user the Employee portal uses.

Answer: A

Explanation:

Adding the employee portal's IP address to the trusted IP range for the connected app is the best way to restrict the connection to Salesforce only to the employee portal server. This will ensure that only requests from the specified IP range will be accepted by Salesforce for that connected app. Option B is not a good choice because using a digital certificate signed by the employee portal server may not be supported by Salesforce for OAuth username-password flow. Option C is not a good choice because adding the employee portal's IP address to the login IP range on the user profile may not be sufficient, as it will still allow other users with the same profile to log in from that IP range. Option D is not a good choice because using a dedicated profile for the user that the employee portal uses may not be effective, as it will still allow other users with that profile to log in from any IP address. References: [Connected Apps], [OAuth 2.0 Username-Password Flow]

NEW QUESTION 47

Which tool should be used to track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours?

- A. Login Inspector
- B. Login History
- C. Login Report
- D. Login Forensics

Answer: D

Explanation:

To track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours,

the identity architect should use Login Forensics. Login Forensics is a tool that analyzes login data and provides insights into user behavior and login patterns. Login Forensics can help identify anomalies, risks, and trends in user login activity. Login Forensics can also generate reports and dashboards to visualize the login data. References: Login Forensics, Analyze Login Data with Login Forensics

NEW QUESTION 50

What are three capabilities of Delegated Authentication? Choose 3 answers

- A. It can be assigned by Custom Permissions.
- B. It can connect to SOAP services.
- C. It can be assigned by Permission Sets.
- D. It can be assigned by Profiles.
- E. It can connect to REST services.

Answer: BCE

Explanation:

The three capabilities of delegated authentication are:

- It can connect to SOAP services. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This feature enables Salesforce to integrate with existing identity stores or authentication methods that support SOAP services.
- It can be assigned by permission sets. Permission sets are collections of settings and permissions that give users access to various tools and functions in Salesforce. Permission sets can be used to assign delegated authentication to users by enabling the "Is Single Sign-on Enabled" permission. This permission allows users to log in with delegated authentication instead of their Salesforce username and password.
- It can connect to REST services. REST services are web services that use HTTP methods to access or manipulate resources on a server. REST services can be used for delegated authentication by creating a custom login page that makes a REST callout to an external service that verifies the user's credentials. This approach requires custom code and configuration, but it provides more flexibility and control over the authentication process.

The other options are not capabilities of delegated authentication. Delegated authentication cannot be assigned by custom permissions or profiles. Custom permissions are settings that can be used in Apex code or validation rules to check whether a user has access to a custom feature or functionality. Custom permissions cannot be used to enable delegated authentication for users. Profiles are collections of settings and permissions that determine what users can do in Salesforce. Profiles cannot be used to enable delegated authentication for users, as this feature is controlled by permission sets. References: [Delegated Authentication], [Permission Sets], [Enable 'Delegated Authentication'], [REST Services], [Custom Login Page for Delegated Authentication], [Custom Permissions], [Profiles]

NEW QUESTION 53

Which two security risks can be mitigated by enabling Two-Factor Authentication (2FA) in Salesforce? Choose 2 answers

- A. Users leaving laptops unattended and not logging out of Salesforce.
- B. Users accessing Salesforce from a public Wi-Fi access point.
- C. Users choosing passwords that are the same as their Facebook password.
- D. Users creating simple-to-guess password reset questions.

Answer: BC

Explanation:

Enabling Two-Factor Authentication (2FA) in Salesforce can mitigate the security risks of users accessing Salesforce from a public Wi-Fi access point or choosing passwords that are the same as their Facebook password. 2FA is an additional layer of protection beyond your password that requires users to verify their identity with another factor, such as a mobile app, a security key, or a verification code. This can prevent unauthorized access even if the user's password is compromised or guessed by a malicious actor. The other options are not directly related to 2FA, but rather to user behavior or password policies.

NEW QUESTION 57

An Identity and Access Management (IAM) architect is tasked with unifying multiple B2C Commerce sites and an Experience Cloud community with a single identity. The solution needs to support more than 1,000 logins per minute.

What should the IAM do to fulfill this requirement?

- A. Configure both the community and the commerce sites as OAuth2 RPs (relying party) with an external identity provider.
- B. Configure community as a Security Assertion Markup Language (SAML) identity provider and enable Just-in-Time Provisioning to B2C Commerce.
- C. Create a default account for capturing all ecommerce contacts registered on the community because person Account is not supported for this case.
- D. Confirm performance considerations with Salesforce Customer Support due to high peaks.

Answer: A

Explanation:

According to the Salesforce documentation², OAuth2 RPs (relying parties) are applications that use OAuth 2.0 for authentication and authorization with an external identity provider. This allows users to log in to multiple applications with a single identity provider account. The identity provider issues an access token to the relying party, which can be used to access protected resources on behalf of the user. This solution can support high volumes of logins per minute and unify multiple B2C Commerce sites and an Experience Cloud community with a single identity.

NEW QUESTION 58

Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers.

How should this functionality be enabled for UC, assuming all social sign-on providers support OpenID Connect?

- A. Configure an authentication provider and a registration handler for each social sign-on provider.
- B. Configure a single sign-on setting and a registration handler for each social sign-on provider.
- C. Configure an authentication provider and a Just-In-Time (JIT) handler for each social sign-on provider.
- D. Configure a single sign-on setting and a JIT handler for each social sign-on provider.

Answer: A

Explanation:

To allow customers to login using Facebook, Google, and other social sign-on providers, the identity architect should configure an authentication provider and a registration handler for each social sign-on provider. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. OpenID Connect is a protocol that allows users to sign in with an external identity provider, such as Facebook or Google, and access Salesforce resources. To enable this, the identity architect needs to configure an OpenID Connect Authentication Provider in Salesforce and link it to a connected app. A registration handler is a class that implements the Auth.RegistrationHandler interface and defines how to create or update users in Salesforce based on the information from the external identity provider. The registration handler can also be used to link the user's social identity with their Salesforce identity and prevent duplicate accounts. References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect, Create a Custom Registration Handler

NEW QUESTION 60

The security team at Universal Containers(UC) has identified exporting reports as a high-risk action and would like to require users to be logged into Salesforce with their active directory (AD) credentials when doing so. For all other uses of Salesforce, Users should be allowed to use AD credentials or Salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with Salesforce credentials?

- A. Use SAML Federated Authentication and Custom SAML JIT provisioning to dynamically add or remove a permission set that grants the Export Reports permission.
- B. Use SAML Federated Authentication, treat SAML sessions as high assurance, and raise the session level required for exporting reports.
- C. Use SAML Federated Authentication and block access to reports when accesses through a standard assurance session.
- D. Use SAML Federated Authentication with a login flow to dynamically add or remove a permission set that grants the export reports permission.

Answer: B

Explanation:

Using SAML Federated Authentication, treating SAML sessions as high assurance, and raising the session level required for exporting reports is the solution that should be recommended. This solution ensures that users can only export reports when they log in using AD credentials, which provide a high level of identity verification. Users who log in using Salesforce credentials, which provide a standard level of security, can still view reports but not export them. To implement this solution, you need to configure SAML Federated Authentication with AD as the identity provider⁴, set the session security level for SAML assertions to high assurance⁵, and require high-assurance session security for exporting reports¹. This solution also avoids the complexity and overhead of creating and managing custom permission sets or login flows.

NEW QUESTION 61

Universal Containers (UC) wants its users to access Salesforce and other SSO-enabled applications from a custom web page that UC manages. UC wants its users to use the same set of credentials to access each of the applications. What SAML SSO flow should an Architect recommend for UC?

- A. SP-Initiated with Deep Linking
- B. SP-Initiated
- C. IdP-Initiated
- D. User-Agent

Answer: C

Explanation:

The SAML SSO flow that an architect should recommend for UC is IdP-initiated. IdP-initiated SSO is a process that allows users to start at the IdP site, such as UC's custom web page, and then be redirected to Salesforce or other SPs with a SAML assertion that contains information about the user's identity and attributes. This flow enables UC to provide a single point of entry for its users to access multiple applications with the same credentials, as they do not need to enter their username and password again for each application. This flow also simplifies the configuration and maintenance of SSO, as UC does not need to create or manage deep links or URLs for each application.

The other options are not valid SAML SSO flows for this scenario. SP-initiated with deep linking is a process that allows users to start at a specific resource on the SP site, such as a report or dashboard, and then be redirected to the IdP for authentication and back to the resource with a SAML assertion. This flow is not suitable for UC's scenario, as they want their users to start at their custom web page, not at a specific resource on Salesforce or other SPs. SP-initiated is a process that allows users to start at the SP site, such as Salesforce or other applications, and then be redirected to the IdP for authentication and back to the SP site with a SAML assertion. This flow is not suitable for UC's scenario, as they want their users to start at their custom web page, not at each application separately. User-agent is not a standard term for SAML SSO, but it could refer to user-agent flow, which is an OAuth authorization flow that allows users to obtain an access token from Salesforce by using a browser or web-view. This flow is not suitable for UC's scenario, as it does not use SAML or IdP for authentication. References: [SAML Single Sign-On], [IdP-Initiated Login], [SP-Initiated Login], [Deep Linking], [OAuth User-Agent Flow]

NEW QUESTION 62

Universal Containers (UC) is successfully using Delegated Authentication for their Salesforce users. The service supporting Delegated Authentication is written in Java. UC has a new CIO that is requiring all company Web services be RESTful and written in .NET. Which two considerations should the UC Architect provide to the new CIO? Choose 2 answers

- A. Delegated Authentication will not work with a .NET service.
- B. Delegated Authentication will continue to work with REST services.
- C. Delegated Authentication will continue to work with a .NET service.
- D. Delegated Authentication will not work with REST services.

Answer: CD

Explanation:

Delegated Authentication will continue to work with a .NET service as long as it is wrapped in a web service that Salesforce can consume¹. Delegated Authentication will not work with REST services because it requires a SOAP-based web service²³. Therefore, option C and D are the correct answers. References: Salesforce Documentation, DEV Community, Salesforce Developer Community

NEW QUESTION 65

Northern Trail Outfitters (NTO) is planning to implement a community for its customers using Salesforce Experience Cloud. Customers are not able to self-register. NTO would like to have customers set their own passwords when provided access to the community. Which two recommendations should an identity architect make to fulfill this requirement? Choose 2 answers

- A. Add customers as contacts and add them to Experience Cloud site.
- B. Enable Welcome emails while configuring the Experience Cloud site.
- C. Allow Password reset using the API to update Experience Cloud site membership.
- D. Use Login Flows to allow users to reset password in Experience Cloud site.

Answer: CD

Explanation:

Allowing password reset using the API and using login flows are two possible ways to enable customers to set their own passwords in Experience Cloud. The other options are not relevant for this requirement, as they do not address the password issue. References: Allow Password Reset Using the API, Use Login Flows to Allow Users to Reset Passwords in Experience Cloud Sites

NEW QUESTION 70

Which two statements are capable of Identity Connect? Choose 2 answers

- A. Synchronization of Salesforce Permission Set Licence Assignments.
- B. Supports both Identity-Provider-Initiated and Service-Provider-Initiated SSO.
- C. Support multiple orgs connecting to multiple Active Directory servers.
- D. Automated user synchronization and de-activation.

Answer: BD

Explanation:

The two statements that are capabilities of Identity Connect are:

➤ It supports both identity-provider-initiated and service-provider-initiated SSO. Identity Connect is a desktop application that integrates Salesforce with Microsoft Active Directory (AD) and enables single sign-on (SSO) between the two systems. Identity Connect supports both identity-provider-initiated SSO, which is when the user starts at the AD site and then is redirected to Salesforce with a SAML assertion, and service-provider-initiated SSO, which is when the user starts at the Salesforce site and then is redirected to AD for authentication.

➤ It enables automated user synchronization and deactivation. Identity Connect allows administrators to synchronize user accounts and attributes between AD and Salesforce, either manually or on a scheduled basis. Identity Connect also allows administrators to deactivate user accounts in Salesforce when they are disabled or deleted in AD, which helps maintain security and compliance.

The other options are not capabilities of Identity Connect. Identity Connect does not support synchronization of Salesforce permission set license assignments, as these are not related to AD attributes. Identity Connect does not support multiple orgs connecting to multiple AD servers, as it can only connect one Salesforce org to one AD domain at a time. References: [Identity Connect], [Identity Connect Features], [Identity Connect User Synchronization], [Identity Connect Single Sign-On]

NEW QUESTION 72

Universal Containers (UC) has five Salesforce orgs (UC1, UC2, UC3, UC4, UC5). of Every user that is in UC2, UC3, UC4, and UC5 is also in UC1, however not all users 65* have access to every org. Universal Containers would like to simplify the authentication process such that all Salesforce users need to remember one set of credentials. UC would like to achieve this with the least impact to cost and maintenance. What approach should an Architect recommend to UC?

- A. Purchase a third-party Identity Provider for all five Salesforce orgs to use and set up JIT user provisioning on all other orgs.
- B. Purchase a third-party Identity Provider for all five Salesforce orgs to use, but don't set up JIT user provisioning for other orgs.
- C. Configure UC1 as the Identity Provider to the other four Salesforce orgs and set up JIT user provisioning on all other orgs.
- D. Configure UC1 as the Identity Provider to the other four Salesforce orgs, but don't set up JIT user provisioning for other orgs.

Answer: C

Explanation:

The best approach to simplify the authentication process and reduce cost and maintenance is to configure UC1 as the Identity Provider to the other four Salesforce orgs and set up JIT user provisioning on all other

orgs. This way, users can log in to any of the five orgs using their UC1 credentials, and their user accounts will be automatically created or updated in the other orgs based on the information from UC1. This eliminates the need to purchase a third-party Identity Provider or manually provision users in advance. The other options are not optimal for this requirement because:

➤ Purchasing a third-party Identity Provider for all five Salesforce orgs would incur additional cost and maintenance, and would not leverage the existing user base in UC1.

➤ Not setting up JIT user provisioning for other orgs would require manually creating or updating user accounts in each org, which would be time-consuming and error-prone. References: Salesforce as an Identity Provider, Identity Providers and Service Providers, Just-in-Time Provisioning for SAML

NEW QUESTION 74

A global fitness equipment manufacturer is planning to sell fitness tracking devices and has the following requirements:

- 1) Customer purchases the device.
 - 2) Customer registers the device using their mobile app.
 - 3) A case should automatically be created in Salesforce and associated with the customer's account in cases where the device registers issues with tracking.
- Which OAuth flow should be used to meet these requirements?

- A. OAuth 2.0 Asset Token Flow
- B. OAuth 2.0 Username-Password Flow
- C. OAuth 2.0 User-Agent Flow
- D. OAuth 2.0 SAML Bearer Assertion Flow

Answer: A

Explanation:

OAuth 2.0 Asset Token Flow is the flow that allows customers to register their devices with Salesforce and get an access token that can be used to create cases. The other flows are not suitable for this use case.

References: OAuth Authorization Flows Trailblazer Community Documentation

NEW QUESTION 76

Universal Containers (UC) wants to build a mobile application that will be making calls to the Salesforce REST API. UC's Salesforce implementation relies heavily on custom objects and custom Apex code. UC does not want its users to have to enter credentials every time they use the app. Which two scope values should an Architect recommend to UC? Choose 2 answers.

- A. Custom_permissions
- B. Api
- C. Refresh_token
- D. Full

Answer: BC

Explanation:

The two scope values that an architect should recommend to UC are api and refresh_token. The api scope allows the app to access the Salesforce REST API and use custom objects and custom Apex code. The refresh_token scope allows the app to obtain a refresh token that can be used to get new access tokens without requiring the user to re-enter credentials. Option A is not a good choice because the custom_permissions scope allows the app to access custom permissions in Salesforce, but it does not affect how the app can access the REST API or avoid user re-authentication. Option D is not a good choice because the full scope allows the app to access all data accessible by the user, including the web UI and the API, but it may be unnecessary or insecure for UC's requirement. References: OAuth 2.0 Web Server Authentication Flow, Digging Deeper into OAuth 2.0 on Force.com

NEW QUESTION 79

Universal Containers (UC) has a mobile application that calls the Salesforce REST API. In order to prevent users from having to enter their credentials everytime they use the app, UC has enabled the use of refresh Tokens as part of the Salesforce connected App and updated their mobile app to take advantage of the refresh token. Even after enabling the refresh token, Users are still complaining that they have to enter their credentials once a day. What is the most likely cause of the issue?

- A. The OAuth authorizations are being revoked by a nightly batch job.
- B. The refresh token expiration policy is set incorrectly in Salesforce
- C. The app is requesting too many access Tokens in a 24-hour period
- D. The users forget to check the box to remember their credentials.

Answer: B

Explanation:

The most likely cause of the issue is that the refresh token expiration policy is set incorrectly in Salesforce. A refresh token is a credential that allows a connected app to obtain a new access token when the previous one expires¹. The refresh token expiration policy determines how long a refresh token is valid for². If the policy is set to a short duration, such as 24 hours, the users have to enter their credentials once a day to get a new refresh token. To prevent this, the policy should be set to a longer duration, such as "Refresh token is valid until revoked" or "Refresh token expires after 90 days of inactivity"². References: OAuth 2.0 Refresh Token Flow, Manage OAuth Access Policies for a Connected App

NEW QUESTION 83

Universal Containers wants to secure its Salesforce APIs by using an existing Security Assertion Markup Language (SAML) configuration supports the company's single sign-on process to Salesforce, Which Salesforce OAuth authorization flow should be used?

- A. OAuth 2.0 SAML Bearer Assertion Flow
- B. A SAML Assertion Row
- C. OAuth 2.0 User-Agent Flow
- D. OAuth 2.0 JWT Bearer Flow

Answer: A

Explanation:

OAuth 2.0 SAML Bearer Assertion Flow allows a client application to use a SAML assertion to request an access token from Salesforce. This flow can leverage the existing SAML configuration for single sign-on and secure the Salesforce APIs. References: OAuth 2.0 SAML Bearer Assertion Flow

NEW QUESTION 85

Universal Containers is implementing Salesforce Identity to broker authentication from its enterprise single sign-on (SSO) solution through Salesforce to third party applications using SAML.

What role does Salesforce Identity play in its relationship with the enterprise SSO system?

- A. Identity Provider (IdP)
- B. Resource Server
- C. Service Provider (SP)
- D. Client Application

Answer: C

Explanation:

To broker authentication from its enterprise SSO solution through Salesforce to third party applications using SAML, Salesforce Identity plays the role of a Service Provider (SP). A SP is an entity that relies on an Identity Provider (IdP) to authenticate and authorize users. In this scenario, the enterprise SSO solution is the IdP, Salesforce is the SP, and the third party applications are the Resource Servers or Client Applications. The SP receives a SAML assertion from the IdP and uses it to obtain an access token from the Resource Server or Client Application. References: SAML Single Sign-On Settings, Authorize Apps with OAuth

NEW QUESTION 90

Universal Containers (UC) is using Active Directory as its corporate identity provider and Salesforce as its CRM for customer care agents, who use SAML based single sign-on to login to Salesforce. The default agent profile does not include the Manage User permission. UC wants to dynamically update the agent role and permission sets.

Which two mechanisms are used to provision agents with the appropriate permissions? Choose 2 answers

- A. Use Login Flow in User Context to update role and permission sets.
- B. Use Login Flow in System Context to update role and permission sets.
- C. Use SAML Just-in-Time (JIT) Handler class run as current user to update role and permission sets.
- D. Use SAML Just-in-Time (JIT) handler class run as an admin user to update role and permission sets.

Answer: BD

Explanation:

To dynamically update the agent role and permission sets using Active Directory as the corporate identity provider and Salesforce as the CRM for customer care agents, who use SAML based sign-on to login to Salesforce, the identity architect should use two mechanisms:

- Use Login Flow in System Context to update role and permission sets. A Login Flow is a custom post-authentication process that can be used to add additional screens or logic after a user logs in to Salesforce. A System Context is a mode that allows a Login Flow to run as an administrator user with full access to Salesforce data and metadata. By using a Login Flow in System Context, the identity architect can update the agent role and permission sets based on the information from Active Directory or other criteria.
- Use SAML Just-in-Time (JIT) handler class run as an admin user to update role and permission sets. A SAML JIT handler class is a class that implements the Auth.SamlJitHandler interface and defines how to handle SAML assertions for Just-in-Time (JIT) provisioning. JIT provisioning is a feature that allows Salesforce to create or update user records on the fly when users log in through an external identity provider. By using a SAML JIT handler class run as an admin user, the identity architect can update the agent role and permission sets based on the information from the SAML assertion. References: Login Flows, SAML Just-in-Time Provisioning, Auth.SamlJitHandler Interface

NEW QUESTION 91

Universal Containers (UC) is using its production org as the identity provider for a new Experience Cloud site and the identity architect is deciding which login experience to use for the site. Which two page types are valid login page types for the site?

Choose 2 answers

- A. Experience Builder Page
- B. lightning Experience Page
- C. Login Discovery Page
- D. Embedded Login Page

Answer: CD

Explanation:

Login Discovery Page and Embedded Login Page are two valid login page types for Experience Cloud sites. Login Discovery Page allows users to choose their preferred login method, such as username/password, SSO, or social sign-on. Embedded Login Page allows users to log in from any site page without being redirected to a separate login page. References: Login Discovery Page, Embedded Login

NEW QUESTION 92

Universal Containers (UC) has an existing web application that it would like to access from Salesforce without requiring users to re-authenticate. The web application is owned UC and the UC team that is responsible for it is willing to add new javascript code and/or libraries to the application. What implementation should an Architect recommend to UC?

- A. Create a Canvas app and use Signed Requests to authenticate the users.
- B. Rewrite the web application as a set of Visualforce pages and Apex code.
- C. Configure the web application as an item in the Salesforce App Launcher.
- D. Add the web application as a ConnectedApp using OAuth User-Agent flow.

Answer: A

Explanation:

A Canvas app is a web application that can be embedded within Salesforce and access Salesforce data using the signed request authentication method. This method allows the Canvas app to receive a signed request that contains the context and OAuth token when it is loaded. The Canvas app can use the SDK to request a new or refreshed signed request on demand². This way, the users do not need to re-authenticate when accessing the web application from Salesforce. References: Requesting a Signed Request, SAML Single Sign-On for Canv Apps, Mastering Salesforce Canvas Apps

NEW QUESTION 95

How should an Architect force user to authenticate with Two-factor Authentication (2FA) for Salesforce only when not connected to an internal company network?

- A. Use Custom Login Flows with Apex to detect the user's IP address and prompt for 2FA if needed.
- B. Add the list of company's network IP addresses to the Login Range list under 2FA Setup.
- C. Use an Apex Trigger on the UserLogin object to detect the user's IP address and prompt for 2FA if needed.
- D. Apply the "Two-factor Authentication for User Interface Logins" permission and Login IP Ranges for all Profiles.

Answer: A

Explanation:

Using Custom Login Flows with Apex is the best option to force users to authenticate with 2FA for Salesforce only when not connected to an internal company network. Custom Login Flows allow admins to customize the login process for different scenarios and user types². Apex code can be used to detect the user's IP address and prompt for 2FA if it is not within the company's network range³. The other options are not suitable because they either do not support 2FA or do not allow conditional logic based on the user's IP address.

NEW QUESTION 96

Universal Containers would like its customers to register and log in to a portal built on Salesforce Experience Cloud. Customers should be able to use their Facebook or LinkedIn credentials for ease of use.

Which three steps should an identity architect take to implement social sign-on? Choose 3 answers

- A. Register both Facebook and LinkedIn as connected apps.
- B. Create authentication providers for both Facebook and LinkedIn.

- C. Check "Facebook" and "LinkedIn" under Login Page Setup.
- D. Enable "Federated Single Sign-On Using SAML".
- E. Update the default registration handlers to create and update users.

Answer: BCE

Explanation:

To implement social sign-on for customers to register and log in to a portal built on Salesforce Experience Cloud using their Facebook or LinkedIn credentials, the identity architect should take three steps:

- Create authentication providers for both Facebook and LinkedIn. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and LinkedIn, which can be easily configured with minimal customization.
- Check "Facebook" and "LinkedIn" under Login Page Setup. Login Page Setup is a setting that allows administrators to customize the login page for Experience Cloud sites. By checking "Facebook" and "LinkedIn", the identity architect can enable social sign-on buttons for these identity providers on the login page.
- Update the default registration handlers to create and update users. Registration handlers are classes that implement the Auth.RegistrationHandler interface and define how to create or update users in Salesforce based on the information from the external identity provider. The identity architect can update the default registration handlers to link the user's social identity with their Salesforce identity and prevent duplicate accounts. References: Authentication Providers, Social Sign-On with Authentication Providers, Login Page Setup, Create a Custom Registration Handler

NEW QUESTION 101

Universal Containers (UC) has an existing Salesforce org configured for SP-Initiated SAML SSO with their Idp. A second Salesforce org is being introduced into the environment and the IT team would like to ensure they can use the same Idp for new org. What action should the IT team take while implementing the second org?

- A. Use the same SAML Identity location as the first org.
- B. Use a different Entity ID than the first org.
- C. Use the same request bindings as the first org.
- D. Use the Salesforce Username as the SAML Identity Type.

Answer: B

Explanation:

The Entity ID is a unique identifier for a service provider or an identity provider in SAML SSO. It is used to differentiate between different service providers or identity providers that may share the same issuer or login URL. In Salesforce, the Entity ID is automatically generated based on the organization ID and can be viewed in the Single Sign-On Settings page¹. If you have a custom domain set up, you can use [https:// \[customDomain\].my.salesforce.com](https://[customDomain].my.salesforce.com) as the Entity ID². If you want to use the same IdP for two Salesforce orgs, you need to use different Entity IDs for each org, otherwise the IdP will not be able to distinguish them and may send incorrect assertions. You can also use different certificates, issuers, or login URLs for each org, but using different Entity IDs is the simplest and recommended way³.

NEW QUESTION 103

Containers (UC) uses a legacy Employee portal for their employees to collaborate. Employees access the portal from their company's internal website via SSO. It is set up to work with SiteMinder and Active Directory. The Employee portal has features to support posing ideas. UC decides to use Salesforce Ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to integrate Employee portal ideas with Salesforce idea through the API. What is the role of Salesforce in the context of SSO, based on this scenario?

- A. Service Provider, because Salesforce is the application for managing ideas.
- B. Connected App, because Salesforce is connected with Employee portal via API.
- C. Identity Provider, because the API calls are authenticated by Salesforce.
- D. An independent system, because Salesforce is not part of the SSO setup.

Answer: D

Explanation:

D is correct because Salesforce is an independent system that is not part of the SSO setup between the Employee portal and Active Directory. Salesforce does not act as an IdP or an SP for the SSO, nor does it use a connected app to integrate with the Employee portal. Salesforce only exposes its API to allow the Employee portal to access its ideas feature.

A is incorrect because Salesforce is not a service provider for the SSO. The SSO is between the Employee portal and Active Directory, not between the Employee portal and Salesforce.

B is incorrect because Salesforce is not a connected app for the SSO. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect¹. The Employee portal does not use any of these protocols to integrate with Salesforce, but only uses its API.

C is incorrect because Salesforce is not an identity provider for the SSO. The IdP is the system that authenticates users and issues tokens or assertions to allow access to other systems. In this scenario, the IdP is Active Directory, not Salesforce.

References: 1: OAuth Authorization flows in Salesforce - Apex Hours

NEW QUESTION 107

Northern Trail Outfitters (NTO) has a requirement to ensure all user logins include a single multi-factor authentication (MFA) prompt. Currently, users are allowed the choice to login with a username and password or via single sign-on against NTO's corporate Identity Provider, which includes built-in MFA. Which configuration will meet this requirement?

- A. Create and assign a permission set to all employees that includes "MFA for User Interface Logins."
- B. Create a custom login flow that enforces MFA and assign it to a permission set
- C. Then assign the permission set to all employees.
- D. Enable "MFA for User Interface Logins" for your organization from Setup -> Identity Verification.
- E. For all employee profiles, set the Session Level Required at Login to High Assurance and add the corporate identity provider to the High Assurance list for the org's Session Security Levels.

Answer: C

Explanation:

Enabling “MFA for User Interface Logins” for the organization is the simplest way to ensure that all user logins include a single MFA prompt. This setting applies to both direct logins and SSO logins, and overrides any other MFA settings at the profile or permission set level. References: Enable MFA for Direct User Logins, Everything You Need to Know About MFA Auto-Enablement and Enforcement

NEW QUESTION 110

Universal Containers (UC) has a Desktop application to collect leads for marketing campaigns. UC wants to extend this application to integrate with Salesforce to create leads. Integration between the desktop application and salesforce should be seamless. What Authorization flow should the Architect recommend?

- A. JWT Bearer Token flow
- B. Web Server Authentication Flow
- C. User Agent Flow
- D. Username and Password Flow

Answer: A

Explanation:

The JWT Bearer Token flow is an OAuth flow in which an external app (also called client or consumer app) sends a signed JSON string to Salesforce called JWT to obtain an access token. The access token can then be used by the external app to read and write data in Salesforce1. This flow is suitable for UC’s scenario because it allows seamless integration between the desktop application and Salesforce without requiring user interaction or login credentials2. The other options are not valid authorization flows for this scenario. The Web Server Authentication Flow and the User Agent Flow both require user interaction and redirection to the Salesforce OAuth authorization endpoint, which is not seamless3. The Username and Password Flow requires the external app to store the user’s login credentials, which is not secure or recommended3.

References: OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration, OAuth Authorization Flows, Salesforce OAuth : JWT Bearer Flow

NEW QUESTION 115

Universal containers (UC) wants to implement Delegated Authentication for a certain subset of Salesforce users. Which three items should UC take into consideration while building the Web service to handle the Delegated Authentication request? Choose 3 answers

- A. The web service needs to include Source IP as a method parameter.
- B. UC should whitelist all salesforce ip ranges on their corporate firewall.
- C. The web service can be written using either the soap or rest protocol.
- D. Delegated Authentication is enabled for the system administrator profile.
- E. The return type of the Web service method should be a Boolean value

Answer: ABE

Explanation:

Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external web service. The web service needs to include the source IP address of the user as a method parameter, so that Salesforce can pass it along with the username and password. UC should whitelist all Salesforce IP ranges on their corporate firewall, so that the web service can accept requests from Salesforce. The return type of the web service method should be a Boolean value, indicating whether the authentication was successful or not. The web service can be written using either SOAP or REST protocol, but this is not a consideration for UC while building the web service. Delegated authentication is not enabled for the system administrator profile, but it can be enabled for other profiles or permission sets. References: Certification - Identity and Access Management Architect - Trailhead, [Delegated Authentication Single Sign-On], [Implementing Single Sign-On Across Multiple Organizations]

NEW QUESTION 116

Universal Containers (UC) wants to implement SAML SSO for their internal of Salesforce users using a third-party IdP. After some evaluation, UC decides NOT to 65« set up My Domain for their Salesforce org. How does that decision impact their SSO implementation?

- A. IdP-initiated SSO will NOT work.
- B. Neither SP- nor IdP-initiated SSO will work.
- C. Either SP- or IdP-initiated SSO will work.
- D. SP-initiated SSO will NOT work

Answer: D

Explanation:

This is because without My Domain, Salesforce will not know in advance what Identity Provider (IdP) to use for SSO, since it does not even know yet what Organization the user is trying to log in to1. SP-initiated SSO is the scenario where the user starts with a Salesforce link (login page, deep link, Outlook Sync URL, etc.) and then gets redirected to the IdP for authentication2. Without My Domain, SP-initiated SSO requires that the user do an IdP-initiated SSO at least once first so that Salesforce can set a cookie in their browser identifying the IdP1. The other options are not correct for this question because:

- IdP-initiated SSO will work without My Domain, as long as the user starts SSO at the IdP and sends the identity information to Salesforce along with SAML protocol information that identifies the Organization and the IdP2.
- Neither SP- nor IdP-initiated SSO will not work is false, as explained above.
- Either SP- or IdP-initiated SSO will work is false, as explained above.

References: Considerations for setting up My Domain and SSO - Salesforce, SAML SSO with Salesforce as the Service Provider

NEW QUESTION 119

Northern Trail Outfitters (NTO) uses Salesforce Experience Cloud sites (previously known as Customer Community) to provide a digital portal where customers can login using their Google account.

NTO would like to automatically create a case record for first time users logging into Salesforce Experience Cloud. What should an Identity architect do to fulfill the requirement?

- A. Configure an authentication provider for Social Login using Google and a custom registration handler.
- B. Implement a Just-in-Time handler class that has logic to create cases upon first login.
- C. Create an authentication provider for Social Login using Google and leverage standard registration handler.
- D. Implement a login flow with a record create component for Case.

Answer: D

Explanation:

To automatically create a case record for first time users logging into Salesforce Experience Cloud using their Google account, the identity architect should implement a login flow with a record create component for Case. A login flow is a custom post-authentication process that can be used to add additional screens or logic after a user logs in to Salesforce. A record create component is a type of flow element that can be used to create a new record in Salesforce. By implementing a login flow with a record create component for Case, the identity architect can check if the user is logging in for the first time using their Google account and create a case record accordingly. References: Login Flows, Record Create Element

NEW QUESTION 123

Universal Containers (UC) is implementing Salesforce and would like to establish SAML SSO for its users to log in. UC stores its corporate user identities in a Custom Database. The UC IT Manager has heard good things about Salesforce Identity Connect as an Idp, and would like to understand what limitations they may face if they decided to use Identity Connect in their current environment. What limitation Should an Architect inform the IT Manager about?

- A. Identity Connect will not support user provisioning in UC's current environment.
- B. Identity Connect will only support Idp-initiated SAML flows in UC's current environment.
- C. Identity Connect will only support SP-initiated SAML flows in UC's current environment.
- D. Identity connect is not compatible with UC's current identity environment.

Answer: A

Explanation:

Identity Connect will not support user provisioning in UC's current environment. Identity Connect is a tool that synchronizes user data between Active Directory and Salesforce, but it does not work with other identity sources such as a Custom Database⁵. Therefore, if UC wants to use Identity Connect as an Idp, they will not be able to provision users from their Custom Database to Salesforce.

Options B, C, and D are incorrect because Identity Connect does not have any limitations on the type of SAML flow or the compatibility with UC's current identity environment. Identity Connect supports both Idp-initiated and SP-initiated SAML flows⁶, and it can act as an Idp for any external service provider that supports SAML 2.0⁷.

References: 5: Identity Connect - Salesforce 6: SAML SSO Flows - Salesforce 7: Salesforce Connect: Integration, Benefits, and Limitations

NEW QUESTION 128

Universal Containers (UC) has an e-commerce website where customers can buy products, make payments, and manage their accounts. UC decides to build a Customer Community on Salesforce and wants to allow the customers to access the community from their accounts without logging in again. UC decides to implement an SP-initiated SSO using a SAML-compliant Idp. In this scenario where Salesforce is the Service Provider, which two activities must be performed in Salesforce to make SP-initiated SSO work? Choose 2 answers

- A. Configure SAML SSO settings.
- B. Create a Connected App.
- C. Configure Delegated Authentication.
- D. Set up My Domain.

Answer: AD

Explanation:

To enable SP-initiated SSO with Salesforce as the Service Provider, two steps are required in Salesforce:

- Option A is correct because configuring SAML SSO settings involves specifying the identity provider details, such as the entity ID, login URL, logout URL, and certificate².
- Option D is correct because setting up My Domain enables you to use a custom domain name for your Salesforce org and allows you to use SAML as an authentication method³.
- Option B is incorrect because creating a connected app is not necessary for SP-initiated SSO using a SAML-compliant IdP. A connected app is used for OAuth-based authentication or OpenID Connect-based authentication⁴.
- Option C is incorrect because configuring delegated authentication is not related to SP-initiated SSO using a SAML-compliant IdP. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service, such as LDAP or Active Directory⁵.

References: SAML-based single sign-on: Configuration and Limitations, Configure SAML single sign-on with an identity provider, My Domain, Create a Connected App, Configure Salesforce for Delegated Authentication

NEW QUESTION 133

Universal Containers (UC) rolling out a new Customer Identity and Access Management Solution will be built on top of their existing Salesforce instance. Several service providers have been setup and integrated with Salesforce using OpenID Connect to allow for a seamless single sign-on experience. UC has a requirement to limit user access to only a subset of service providers per customer type. Which two steps should be done on the platform to satisfy the requirement? Choose 2 answers

- A. Manage which connected apps a user has access to by assigning authentication providers to the user's profile.
- B. Assign the connected app to the customer community, and enable the users profile in the Community settings.
- C. Use Profiles and Permission Sets to assign user access to Admin Pre-Approved Connected Apps.
- D. Set each of the Connected App access settings to Admin Pre-Approved.

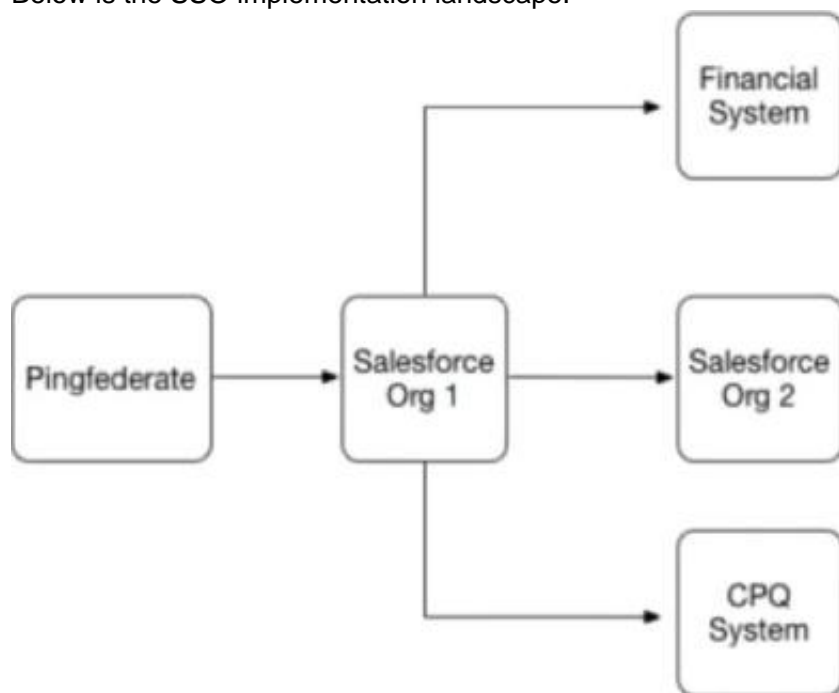
Answer: CD

Explanation:

To limit user access to only a subset of service providers per customer type, the identity architect should use Profiles and Permission Sets to assign user access to Admin Pre-Approved Connected Apps. Connected apps are frameworks that enable external applications to integrate with Salesforce using APIs and standard protocols, such as OpenID Connect. By setting each of the Connected App access settings to Admin Pre-Approved, the identity architect can control which users can access which connected apps by assigning profiles or permission sets to the connected apps. The other options are not relevant for this scenario. References: Connected Apps, Manage Connected Apps

NEW QUESTION 135

Universal Containers (UC) has implemented SAML-based Single Sign-On to provide seamless access to its Salesforce Orgs, financial system, and CPQ system. Below is the SSO implementation landscape.



What role combination is represented by the systems in this scenario"

- A. Financial System and CPQ System are the only Service Providers.
- B. Salesforce Org1 and Salesforce Org2 are the only Service Providers.
- C. Salesforce Org1 and Salesforce Org2 are acting as Identity Providers.
- D. Salesforce Org1 and PingFederate are acting as Identity Providers.

Answer: B

Explanation:

In a SAML-based SSO scenario, the identity provider (IdP) is the system that performs authentication and passes the user's identity and authorization level to the service provider (SP), which trusts the IdP and authorizes the user to access the requested resource¹. In this case, PingFederate is the IdP that authenticates users for UC and sends SAML assertions to the SPs. The SPs are the systems that rely on PingFederate for authentication and provide access to their services based on the SAML assertions. The SPs in this scenario are Salesforce Org1, Salesforce Org2, Financial System, and CPQ System². Therefore, the correct answer is B.

References:

- > SAML web-based authentication guide
- > SAML-based single sign-on: Configuration and Limitations

NEW QUESTION 139

An identity architect is implementing a mobile-first Consumer Identity Access Management (CIAM) for external users. User authentication is the only requirement. The users email or mobile phone number should be supported as a username. Which two licenses are needed to meet this requirement? Choose 2 answers

- A. External Identity Licenses
- B. Identity Connect Licenses
- C. Email Verification Credits
- D. SMS verification Credits

Answer: AD

Explanation:

External Identity Licenses are required to enable external users to access Salesforce resources via a CIAM solution. Email Verification Credits and SMS Verification Credits are required to enable email or mobile phone number verification for user authentication. Identity Connect Licenses are not required for this scenario, as Identity Connect is a tool for synchronizing user data between Salesforce and Active Directory.

References: External Identity Implementation Guide, Identity Connect Implementation Guide

NEW QUESTION 142

Universal Containers wants to implement Single Sign-on for a Salesforce org using an external Identity Provider and corporate identity store. What type of authentication flow is required to support deep linking'

- A. Web Server OAuth SSO flow
- B. Service-Provider-Initiated SSO
- C. Identity-Provider-initiated SSO
- D. StartURL on Identity Provider

Answer: B

Explanation:

Single sign-on (SSO) is an authentication method that enables users to access multiple applications with one login and one set of credentials⁴. There are two types of SSO flows that can be used with Salesforce as the service provider (SP) and an external identity provider (IdP)⁵:

- > Service-provider-initiated SSO: The user requests a resource from the SP, such as a Salesforce URL. The SP redirects the user to the IdP for authentication. The IdP authenticates the user and sends a SAML response to the SP. The SP validates the SAML response and grants access to the user⁵. This type of SSO flow supports deep linking, which means that the user can access a specific page within Salesforce without logging in again⁶.
- > Identity-provider-initiated SSO: The user logs in to the IdP and selects an app from a list of available apps. The IdP sends a SAML response to the SP. The SP validates the SAML response and grants access to the user⁵. This type of SSO flow does not support deep linking, which means that the user can only access the default landing page of Salesforce⁶.

References:

- Single Sign-On
- SAML SSO Flows
- Deep Linking

NEW QUESTION 147

Universal Containers (UC) has a Customer Community that uses Facebook for of authentication. UC would like to ensure that changes in the Facebook profile are reflected on the appropriate Customer Community user. How can this requirement be met?

- A. Use SAML Just-In-Time Provisioning between Facebook and Salesforce.
- B. Use information in the Signed Request that is received from Facebook.
- C. Develop a scheduled job that calls out to Facebook on a nightly basis.
- D. Use the update User () method on the Registration Handler class.

Answer: D

Explanation:

The update User() method on the Registration Handler class is used to update the Salesforce user record with information from the Facebook profile, such as name, email, and photo¹. This method is invoked every time a user logs in to Salesforce using Facebook credentials². The other options are not suitable for this requirement because:

- SAML Just-In-Time Provisioning is used to create or update users in Salesforce based on SAML assertions from an identity provider³. Facebook does not support SAML as an identity provider.
- The Signed Request is a parameter that contains information about the user who is logging in to Salesforce via Facebook. It does not contain the user's profile information, such as name, email, or photo.
- A scheduled job that calls out to Facebook on a nightly basis would not reflect the changes in the Facebook profile in real time, as the requirement states. It would also require storing the user's Facebook access token and making API calls to Facebook, which could be inefficient and insecure. References: Set Up Social Sign-On, Configure a Facebook Authentication Provider, SAML Just-in-Time Provisioning, [Facebook as a SAML Identity Provider], [Facebook Login for Apps - Signed Request], [Facebook Login for Apps - Access Tokens], [Facebook Graph API - User]

NEW QUESTION 149

Universal Containers (UC) wants to build a custom mobile app for their field reps to create orders in salesforce. After the first time the users log in, they must be able to access salesforce upon opening the mobile app without being prompted to log in again. What Oauth flows should be considered to support this requirement?

- A. Web Server flow with a Refresh Token.
- B. Mobile Agent flow with a Bearer Token.
- C. User Agent flow with a Refresh Token.
- D. SAML Assertion flow with a Bearer Token.

Answer: AC

Explanation:

The OAuth 2.0 user-agent flow and the OAuth 2.0 web server flow are both suitable for building a custom mobile app that can access Salesforce data without prompting the user to log in again¹. Both of these flows use a refresh token that can be used to obtain a new access token when the previous one expires². The user-agent flow uses the Canvas JavaScript SDK to obtain an OAuth token by using the login function in the SDK². The web server flow redirects the user to the Salesforce OAuth authorization endpoint and then obtains an OAuth access token by making a POST request to the Salesforce OAuth token endpoint². The mobile agent flow and the SAML assertion flow are not valid OAuth flows for Salesforce³.

References: OAuth Authorization Flows, Mastering Salesforce Canvas Apps, Access Data with API Integration

NEW QUESTION 154

Universal containers wants to set up SSO for a selected group of users to access external applications from salesforce through App launcher. Which three steps must be completed in salesforce to accomplish the goal?

- A. Associate user profiles with the connected Apps.
- B. Complete my domain and Identity provider setup.
- C. Create connected apps for the external applications.
- D. Complete single Sign-on settings in security controls.
- E. Create named credentials for each external system.

Answer: ABC

Explanation:

To set up SSO for a selected group of users to access external applications from Salesforce through App Launcher, UC must complete the following steps in Salesforce:

- Associate user profiles with the connected apps. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect³. To access a connected app, users must have the appropriate permissions assigned to them, either through their profile or a permission set⁴. UC can associate user profiles with the connected apps to control which users can access which apps.
- Complete My Domain and identity provider setup. My Domain is a feature that lets UC create a custom domain name for their Salesforce org. It is required for setting up SSO with external identity providers. An identity provider is a trusted system that authenticates users for other service providers. UC must set up an identity provider that supports SSO protocols such as SAML or OpenID Connect and configure it to communicate with Salesforce.
- Create connected apps for the external applications. UC must create connected apps for each external application that they want to access from Salesforce through App Launcher. A connected app defines the attributes of the external application, such as its name, logo, description, and callback URL⁴. It also specifies the SSO protocol and settings that are used to authenticate users and grant access tokens⁴.
- References: Learn About Connected Apps, Create a Connected App, [Set Up My Domain], Single Sign-On, [Identity Providers and Service Providers]

NEW QUESTION 158

Universal Containers (UC) uses Active Directory (AD) as their identity store for employees and must continue to do so for network access. UC is undergoing a major transformation program and moving all of their enterprise applications to cloud platforms including Salesforce, Workday, and SAP HANA. UC needs to implement an SSO solution for accessing all of the third-party cloud applications and the CIO is inclined to use Salesforce for all of their identity and access management needs.

Which two Salesforce license types does UC need for its employees' Choose 2 answers

- A. Company Community and Identity licenses
- B. Identity and Identity Connect licenses
- C. Chatter Only and Identity licenses
- D. Salesforce and Identity Connect licenses

Answer: BD

Explanation:

The two Salesforce license types that UC needs for its employees are Identity and Identity Connect licenses. According to the Salesforce documentation, "Identity licenses let your employees access any app that supports standards-based single sign-on (SSO). Identity Connect licenses let you integrate your Active Directory with Salesforce." Therefore, option B and D are the correct answers. References: [Identity Licenses]

NEW QUESTION 163

How should an identity architect automate provisioning and deprovisioning of users into Salesforce from an external system?

- A. Call SOAP API upsertQ on user object.
- B. Use Security Assertion Markup Language Just-in-Time (SAML JIT) on incoming SAML assertions.
- C. Run registration handler on incoming OAuth responses.
- D. Call OpenID Connect (OIDC)-userinfo endpoint with a valid access token.

Answer: C

Explanation:

To automate provisioning and deprovisioning of users into Salesforce from an external system, the identity architect should run a registration handler on incoming OAuth responses. A registration handler is a class that implements the Auth.RegistrationHandler interface and defines how to create or update users in Salesforce based on the information from an external identity provider. OAuth is a protocol that allows users to authorize an external application to access Salesforce resources on their behalf. By running a registration handler on incoming OAuth responses, the identity architect can automate user provisioning and deprovisioning based on the OAuth attributes. References: Registration Handler, Authorize Apps with OAuth

NEW QUESTION 167

Northern Trail Outfitters is implementing a business-to-business (B2B) collaboration site using Salesforce Experience Cloud. The partners will authenticate with an existing identity provider and the solution will utilize Security Assertion Markup Language (SAML) to provide single sign-on to Salesforce. Delegated administration will be used in the Expenence Cloud site to allow the partners to administer their users' access.

How should a partner identity be provisioned in Salesforce for this solution?

- A. Create only a contact.
- B. Create a contactless user.
- C. Create a user and a related contact.
- D. Create a person account.

Answer: C

Explanation:

To provision a partner identity in Salesforce for a B2B collaboration site using SAML SSO, the identity architect should create a user and a related contact. A user record is required to authenticate and authorize the partner to access Salesforce resources. A contact record is required to associate the partner with an account, which represents the partner's organization. A contactless user or a person account are not supported for B2B collaboration sites. References: User and Contact Records for Partner Users, Create Partner Users

NEW QUESTION 171

Universal Containers (UC) wants its closed Won opportunities to be synced to a Data Warehouse in near real time. UC has implemented Outbound Message to enable near real-time data sync. UC wants to ensure that communication between Salesforce and Target System is Secure. What Certificate is sent along with the Outbound Message?

- A. The CA-Signed Certificate from the Certificate and Key Management menu.
- B. The default Client Certificate from the Develop--> API Menu.
- C. The default Client Certificate or a Certificate from Certificate and Key Management menu.
- D. The Self-Signed Certificates from the Certificate & Key Management menu.

Answer: A

Explanation:

The CA-Signed Certificate from the Certificate and Key Management menu is the certificate that is sent along with the outbound message. An outbound message is a SOAP message that is sent from Salesforce to an external endpoint when a workflow rule or approval process is triggered. To ensure that the communication between Salesforce and the target system is secure, the outbound message can be signed with a certificate that is generated or uploaded in the Certificate and Key Management menu. The certificate must be CA-Signed, which means that it is issued by a trusted certificate authority (CA) that verifies the identity of the sender. The other options are not valid certificates for this purpose. The default client certificate from the Develop--> API Menu is a self-signed certificate that is used for testing purposes only and does not provide adequate security. The default client certificate or a certificate from Certificate and Key Management menu is too vague and does not specify whether the certificate is CA-Signed or self-signed. The self-signed certificates from the Certificate & Key Management menu are certificates that are generated by Salesforce without any verification by a CA, and they are not recommended for production use.

References: [Outbound Messages], [Sign Outbound Messages with a Certificate], [CA-Signed Certificates], [Default Client Certificate], [Self-Signed Certificates]

NEW QUESTION 175

Universal Containers (UC) plans to use a SAML-based third-party IdP serving both of the Salesforce Partner Community and the corporate portal. UC partners will log in 65* to the corporate portal to access protected resources, including links to Salesforce resources. What would be the recommended way to configure the IdP so that seamless access can be achieved in this scenario?

- A. Set up the corporate portal as a Connected App in Salesforce and use the Web server OAuth flow.
- B. Configure SP-initiated SSO that passes the SAML token upon Salesforce resource access request.
- C. Set up the corporate portal as a Connected App in Salesforce and use the User Agent OAuth flow.
- D. Configure IdP-initiated SSO that passes the SAML token upon Salesforce resource access request.

Answer: D

Explanation:

The recommended way to configure the IdP for seamless access is to use IdP-initiated SSO that passes the SAML token upon Salesforce resource access request. This means that the user logs in to the corporate portal first, and then clicks a link to access a Salesforce resource. The IdP sends a SAML response to Salesforce with the user's identity and other attributes. Salesforce verifies the SAML response and logs in the user to the appropriate Salesforce org and community¹². This way, the user does not have to log in again to Salesforce or enter any credentials³. References: 1: SAML SSO with Salesforce as the Service Provider 2: Set Up Single Sign-On for Your Internal Users Unit | Salesforce - Trailhead 3: What is IdP-Initiated Single Sign-On? – OneLogin

NEW QUESTION 177

Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow. Application users will authenticate using username and password. They should not be forced to approve API access in the mobile app or reauthenticate for 3 months.

Which two connected app options need to be configured to fulfill this use case?

Choose 2 answers

- A. Set Permitted Users to "Admin approved users are pre-authorized".
- B. Set Permitted Users to "All users may self-authorize".
- C. Set the Session Timeout value to 3 months.
- D. Set the Refresh Token Policy to expire refresh token after 3 months.

Answer: BD

Explanation:

To fulfill the use case of creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow, where users will authenticate using username and password and not be forced to approve API access or reauthenticate for 3 months, the identity architect should configure two connected app options:

- Set Permitted Users to "All users may self-authorize". Permitted Users is a setting that controls how users can access a connected app. By setting it to "All users may self-authorize", the identity architect can allow users to access the connected app without requiring administrator approval or API access confirmation.
- Set the Refresh Token Policy to expire refresh token after 3 months. Refresh Token Policy is a setting that controls how long a refresh token can be used to obtain a new access token without requiring user authentication. By setting it to expire refresh token after 3 months, the identity architect can allow users to access the connected app for 3 months without reauthenticating, as long as they use the app at least once every 90 days. References: Connected Apps, OAuth 2.0 User-Agent Flow

NEW QUESTION 180

The security team at Universal Containers (UC) has identified exporting reports as a high-risk action and would like to require users to be logged into Salesforce with their Active Directory (AD) credentials when doing so. For all other users of Salesforce, users should be allowed to use AD Credentials or Salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with Salesforce credentials?

- A. Use SAML Federated Authentication and block access to reports when accessed through a Standard Assurance session.
- B. Use SAML Federated Authentication and Custom SAML JIT Provisioning to dynamically add or remove a permission set that grants the Export Reports Permission.
- C. Use SAML federated Authentication, treat SAML Sessions as High Assurance, and raise the session level required for exporting reports.
- D. Use SAML federated Authentication with a Login Flow to dynamically add or remove a Permission Set that grants the Export Reports Permission.

Answer: C

Explanation:

The best solution to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with Salesforce credentials is to use SAML federated authentication, treat SAML sessions as high assurance, and raise the session level required for exporting reports. SAML federated authentication is a process that allows users to log in to Salesforce with an external identity provider (IdP), such as AD, that authenticates the user and issues a security token to Salesforce. By treating SAML sessions as high assurance, Salesforce assigns a higher level of trust and security to the sessions that are established by SAML federated authentication. By raising the session level required for exporting reports, Salesforce requires users to have a high assurance session before they can export reports. This solution ensures that only users who log in with AD credentials can export reports, while users who log in with Salesforce credentials can still view reports but not export them.

The other options are not valid solutions for this scenario. Using SAML federated authentication and blocking access to reports when accessed through a standard assurance session would prevent users who log in with Salesforce credentials from viewing reports at all, which is not the desired outcome. Using SAML federated authentication and custom SAML JIT provisioning to dynamically add or remove a permission set that grants the export reports permission would require UC to write custom code and logic to implement the JIT provisioning and manage the permission set, which could increase complexity and cost. Using SAML federated authentication with a login flow to dynamically add or remove a permission set that grants the export reports permission would also require UC to write custom code and logic to implement the login flow and manage the permission set, which could introduce errors and performance issues. References: [SAML Single Sign-On], [Session Security Levels], [Set Session Security Levels for Your Org], [Just-in-Time Provisioning for SAML], [Login Flows]

NEW QUESTION 181

An architect has successfully configured SAML-BASED SSO for universal containers. SSO has been working for 3 months when Universal containers manually adds a batch of new users to salesforce. The new users receive an error from salesforce when trying to use SSO. Existing users are still able to successfully use SSO to access salesforce. What is the probable cause of this behaviour?

- A. The administrator forgot to reset the new user's salesforce password.
- B. The Federation ID field on the new user records is not correctly set

- C. The my domain capability is not enabled on the new user's profile.
- D. The new users do not have the SSO permission enabled on their profiles.

Answer: B

Explanation:

The Federation ID field on the new user records is not correctly set is the probable cause of this behavior. The Federation ID is an additional field contained in the Salesforce interface that allows admins to pick whatever username or username format they want to pass to Salesforce from their user directory for single sign-on. This field does not appear on the user page layout editor or on the user record page by default, and it must be populated with a unique value that matches the identity provider's assertion for each user. If the Federation ID is missing or incorrect, the SSO will fail. The administrator does not need to reset the new user's Salesforce password, as SSO bypasses the password authentication. The My Domain capability is not enabled on the new user's profile, but on the org level, so it does not affect individual users. The new users do not have the SSO permission enabled on their profiles is not a valid option, as there is no such permission in Salesforce.

References: Certification - Identity and Access Management Architect - Trailhead, Federation ID field on Us detail page is not visible, What is the purpose of Salesforce SSO by federation ID?

NEW QUESTION 186

Containers (UC) has an existing Customer Community. UC wants to expand the self-registration capabilities such that customers receive a different community experience based on the data they provide during the registration process. What is the recommended approach an Architect Should recommend to UC?

- A. Create an After Insert Apex trigger on the user object to assign specific custom permissions.
- B. Create separate login flows corresponding to the different community user personas.
- C. Modify the Community pages to utilize specific fields on the User and Contact records.
- D. Modify the existing Communities registration controller to assign different profiles.

Answer: C

Explanation:

The recommended approach for UC to expand the self-registration capabilities such that customers receive a different community experience based on the data they provide during the registration process is to modify the community pages to utilize specific fields on the user and contact records. This approach allows UC to customize the community pages based on the user's profile, preferences, interests, or other attributes that are stored in the user or contact fields. For example, UC can use conditional visibility rules or audience criteria to display different components or content based on the user's field values. This approach does not require any code or complex configuration, and it provides a flexible and personalized community experience for different customer segments. The other options are not recommended for this scenario. Creating an after-insert Apex trigger on the user object to assign specific custom permissions would require UC to write code and manage custom permissions, which could increase maintenance and testing efforts. Creating separate login flows corresponding to the different community user personas would require UC to create multiple login pages and logic, which could increase complexity and confusion. Modifying the existing communities' registration controller to assign different profiles would require UC to write code and manage multiple profiles, which could increase security and governance risks. References: [Customize Your Community Pages], [Set Component Visibility], [Create Custom Login Flows], [Customize Self-Registration]

NEW QUESTION 191

An identity architect wants to secure Salesforce APIs using Security Assertion Markup Language (SAML). For security purposes, administrators will need to authorize the applications that will be consuming the APIs. Which Salesforce OAuth authorization flow should be used?

- A. OAuth 2-0 SAML Bearer Assertion Flow
- B. OAuth 2.0 JWT Bearer Flow
- C. SAML Assertion Flow
- D. OAuth 2.0 User-Agent Flow

Answer: C

Explanation:

OAuth 2.0 SAML Bearer Assertion Flow is a protocol that allows a client app to obtain an access token from Salesforce by using a SAML assertion instead of an authorization code. The SAML assertion contains information about the client app and the user who wants to access Salesforce APIs. To use this flow, the client app needs to have a connected app configured in Salesforce with the Use Digital Signature option enabled and the "api" OAuth scope assigned. The administrators can authorize the applications that will be consuming the APIs by setting the Permitted Users policy of the connected app to Admin approved users are pre-authorized and assigning profiles or permission sets to the connected app. References: OAuth 2.0 SAML Bearer Assertion Flow, Connected Apps, OAuth Scopes

NEW QUESTION 192

Universal containers (UC) has a mobile application that it wants to deploy to all of its salesforce users, including customer Community users. UC would like to minimize the administration overhead, which two items should an architect recommend? Choose 2 answers

- A. Enable the "Refresh Tokens is valid until revoked " setting in the Connected App.
- B. Enable the "Enforce Ip restrictions" settings in the connected App.
- C. Enable the "All users may self-authorize" setting in the Connected App.
- D. Enable the "High Assurance session required" setting in the Connected App.

Answer: AC

Explanation:

The two items that an architect should recommend for UC to minimize the administration overhead are:

➤ Enable the "Refresh Tokens is valid until revoked" setting in the Connected App. This setting allows the mobile app to obtain a refresh token from Salesforce when it obtains an access token. A refresh token can be used to obtain a new access token when the previous one expires or becomes invalid. By enabling this setting in the Connected App, UC can reduce the number of login prompts and authentication failures for its mobile users, as they can use the refresh token to renew their access without entering their credentials again.

➤ Enable the "All users may self-authorize" setting in the Connected App. This setting allows users to grant access to the mobile app without administrator approval. By enabling this setting in the Connected App, UC can simplify and speed up the deployment process for its mobile app, as they do not need to manually authorize each user or group of users.

The other options are not recommended items for this scenario. Enabling the “Enforce IP restrictions” setting in the Connected App would limit the mobile app access to certain IP ranges, which could prevent some users from accessing the app from different locations or networks. Enabling the “High Assurance session required” setting in the Connected App would require users to verify their identity with a second factor before accessing the mobile app, which could increase complexity and inconvenience for users. References: [Connected Apps], [Refresh Token], [All Users May Self-Authorize], [IP Restrictions for Connected Apps], [Require a Second Factor of Authentication for Connected Apps]

NEW QUESTION 196

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Identity-and-Access-Management-Architect Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Identity-and-Access-Management-Architect Product From:

<https://www.2passeasy.com/dumps/Identity-and-Access-Management-Architect/>

Money Back Guarantee

Identity-and-Access-Management-Architect Practice Exam Features:

- * Identity-and-Access-Management-Architect Questions and Answers Updated Frequently
- * Identity-and-Access-Management-Architect Practice Questions Verified by Expert Senior Certified Staff
- * Identity-and-Access-Management-Architect Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * Identity-and-Access-Management-Architect Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year